

Merkblatt: Richtiges Handeln im Betrugsfall

Sollten Sie bemerkt haben, dass Sie persönliche Daten zu Ihrem E-Banking wie Passwörter oder Sicherheitscodes bekannt gegeben haben oder diese verwendet worden sind, empfehlen wir Ihnen folgende Schritte zu unternehmen:

1. Schritt

Sperren Sie Ihren E-Banking-Vertrag, indem Sie auf unserer Loginseite www.onba.ch Ihre Vertragsnummer eingeben und ein fehlerhaftes Passwort. Anschliessend erscheinen Ihnen unten links zwei neue Buttons, klicken Sie auf «Vertrag sperren». Geben Sie Ihr Geburtsdatum ein und klicken Sie auf «Sperren».

The image shows two screenshots of the St. Galler Kantonbank website. The top screenshot displays the 'Passwort bestellen' (Order password) page. It features a header with 'Heute E-Banking.' and 'Morgen Rundum-Service.' with a call to action 'Jetzt entdecken unter sgkb.ch/rundum'. Below this is a contact line: 'E-Banking Help Line 0844 88 44 88 Montag bis Freitag, 07:30 bis 17:30 Uhr'. The main content area is titled 'Passwort bestellen' and includes the instruction: 'Senden Sie mir per eingeschriebener Post ein neues E-Banking Passwort. Das bestehende Passwort für diese Vertragsnummer verliert mit dieser Bestellung seine Gültigkeit.' There are two input fields: 'Vertragsnummer' with the value '1000001' and 'Geburtsdatum' with the value '01.01.1975'. At the bottom are two buttons: 'Abbrechen' and 'Bestellen'.

The bottom screenshot shows the 'Login' page. It has a header with 'Heute E-Banking.' and 'Morgen Rundum-Service.' with the same call to action. The contact line is identical. The main content area is titled 'Login' and has two input fields: 'Vertragsnummer' with the value '100001' and 'Passwort'. At the bottom are two buttons: 'Zurücksetzen' and 'Weiter'. To the right of the login form is a red warning message: 'Ungültige Eingaben' (Invalid input) with the text: 'Die Vertragsnummer oder das Passwort ist nicht korrekt. Bitte kontrollieren Sie ihre Eingaben.' Below this message are two buttons: 'Passwort vergessen' and 'Vertrag sperren'.

2. Schritt

Verändern Sie nach einer Betrugsattacke die betroffene Infrastruktur (Smartphone/PC/Laptop) nicht. Wir bitten Sie weder Installationen noch Deinstallationen durchzuführen und die Geräte für Abklärungszwecke bereit zu halten.

3. Schritt

Wenden Sie sich nach einer Betrugsattacke an die SGKB Help Line (Montag bis Freitag, von 07.30 bis 17.30 Uhr) oder ausserhalb der Geschäftszeiten an info@sgkb.ch und teilen Sie uns den Ablauf des Betrugs mit. Halten Sie Ihre E-Banking Vertragsnummer bereit. Leiten Sie der SGKB suspekten E-Mail-Anfragen an info@sgkb.ch weiter.

4. Schritt

Erstatten Sie eine Strafanzeige bei der örtlichen Polizeistelle. Orientieren Sie die SGKB über die eingereichte Strafanzeige (mit dem zuständigen Beamten und Polizeistelle).

5. Schritt

Da die Zugangsdaten Ihres bestehenden E-Banking-Vertrages entwendet worden sind, empfehlen wir Ihnen aus Sicherheitsgründen den betroffenen Vertrag löschen zu lassen und einen neuen zu eröffnen. Bitte kontaktieren Sie diesbezüglich die SGKB Help Line.